
Penetration Testing Wireless Networks

SANS Assessing Wireless Excerpts
Regarding Penetration Testing

jims@bluenotch.com

Introduction

- Wireless networks are everywhere
 - The perimeter of a network extends beyond classic perimeter firewalls
- Rogue wireless weakens any network
- Wireless equipment is cheap
- Threat exists regardless of wireless policy
- Wireless assessment/pentest necessary

Useful Tools



Wireshark - Open source



Kismet - Open source

Spectrum Analyzer – Hardware



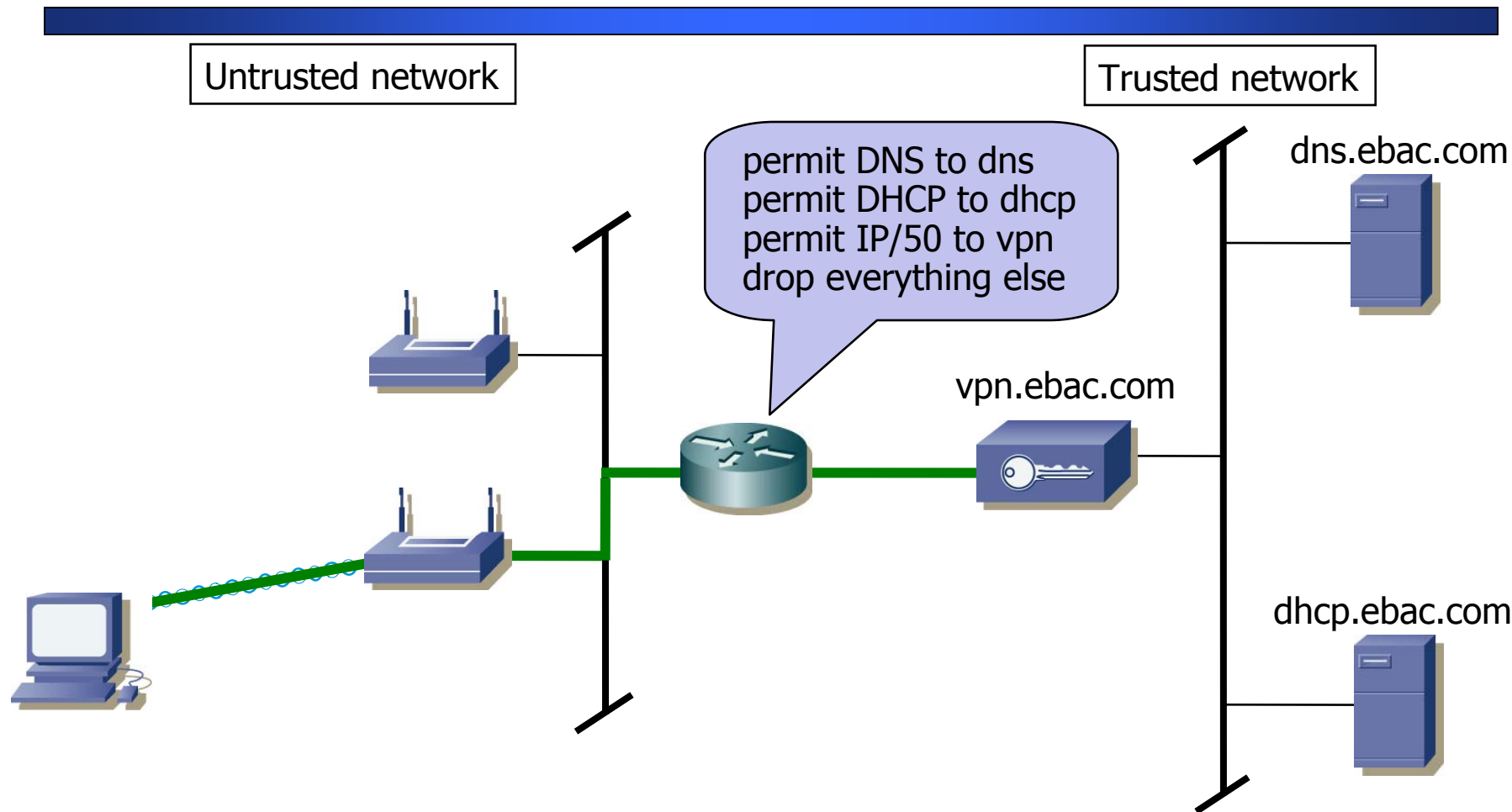
Aircrack-ng - Open source



cowpatty - Open source



Typical Network Deployment



Identifying Wireless

- War-walking/driving/flying
- Use best consumer hardware
 - Favorite 500 mw Alfa USB + 9 dbi
- Linux (drivers support RFMON)
- Look for Rogue Access Points
 - Power/Channel/SSID
 - Triangulate location to highest power

Identifying Wireless (2)

- Focus on 802.11 a/b/g
 - Non-802.11 wireless exists
 - Non FCC channels exists
 - 802.11 – channels 12-14
- Warwalk only identifies live issues
- Some wireless IDS tech helps
- Easy to create an AP from a laptop

Useful Encryption Terms

- RFMON – 802.11 wireless monitor mode
- WEP – Weakest 802.11 encryption
- WPA – Use WEP hardware “better”
- WPA2 – Best 802.11 encryption
- IPSec – Encrypting all IP packets

WEP Issues

- 24 bits of the key don't count (64=40)
- Confidentiality, not Authorization
- Applies to data frames, payload only
- Extremely vulnerable
 - Weak initialization
 - No replay protection
 - Can recover WEP key from plaintext and cyphertext

Attacking WEP

- Weak Initialization Vectors (IVs)
- After enough packets/time, can crack
- Can accelerate with replay of known-plaintext
 - ARP, Windows DHCP, etc.
- wep_crack/WEPAAttack guess WEP key
- Aircrack-ng/Airreplay-ng uses FMS/PTW to crack and accelerate key

FMS Attacks

Aircrack-ng

- Recognizes 5.5 million weak IVs
 - Effective against IV-filtered networks
- Extended with Pychkine, Tews, Weinmann (PTW) attack using ARP response data
- Optimal 104-bit key recovery probability:
 - 50% success after 40,000 packets (60 sec)
 - 80% success after 60,000 packets (90 sec)
 - 95% success after 85,000 packets (128 sec)


Dynamic vs. Static WEP

- DWEP enhances security through dynamic key selection
 - Users authenticate using 802.1X and an EAP type
- Keys are unique per-user and per-session
- Eliminates key selection attacks, vulnerable to many other attacks

Cisco DWEP

- No support to rotate unicast keys via EAPOL-Key messages
- Group keys can be rotated
 - Not enabled by default
- Must force reauthentication to rotate keys
 - Results in ~3-5 second loss of connectivity

```
ap1200#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
ap1200(config)#int dot11Radio 0
ap1200(config-if)#broadcast-key change 600
ap1200(config-if)#dot1x reauth-period 600
```



Where is WEP Vulnerable?

- WEP networks are not only vulnerable at AP location
- Clients can be exploited by impersonating AP, ARP flooding
 - Caffe Latte attack; attacker impersonates a WEP network while victim enjoys coffee
- Keys realistically compromised in ~6 minutes with one client

Method for Cracking WEP (1)

- Capture a few data packets, try wep_crack Neesus Datacom attack
- Next, try dictionary attack with WepAttack
- Start collecting data for Aircrack-ng attack
 - Stop and restart Airodump after ~60,000 data packets
 - Try to recover key while capturing

Method for Cracking WEP (2)

- Use chopchop attack in aireplay-ng to decrypt one packet
 - Learn IP addresses in decrypted content
- Forge an ARP request frame with packetforge-ng
- Replay with aireplay-ng to accelerate IV collection

Wouldn't it be nice if this were automated for us?

wesside-ng

1. Channel hops to find a network
2. Authenticates or impersonates a station
3. Recovers 128-bytes of PRGA/LKE
4. Decrypts a frame to identify network IP information
5. Creates an ARP request for target IP
6. Floods network with ARP requests
7. Launches PTW attack using aircrack-ng

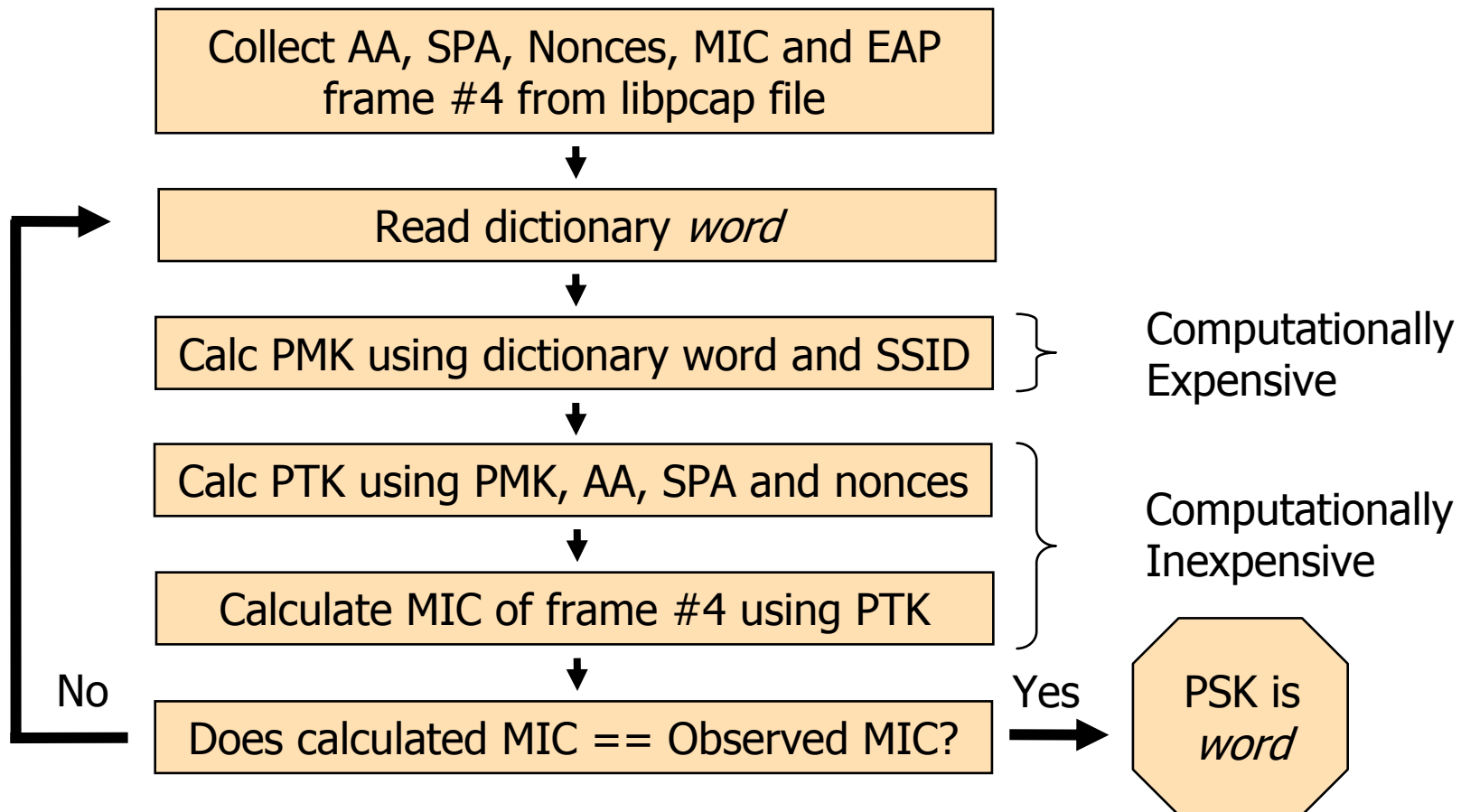
```
Attacker: "./wesside-ng -i ath0"
```


Introduction to WPA

- Portion of 802.11i to secure existing wireless technology
- Moniker for multiple security mechanisms (TKIP)
- Designed to fit with existing hardware
- Based on RC4 encryption, like WEP

Software upgradeable, Paucity of processing cycles

Cowpatty Process



Cowpatty Example

- Requires four-way, wordlist, SSID
- Sample below on Pentium 4 2.8 GHz

```
$ cowpatty -r eapfourway.dump -f passlist -s GNIPGNOPWLAN
```

```
cowpatty 1.2 - WPA-PSK dictionary attack. <jwright@hasborg.com>  
Collected all necessary data to mount crack against passphrase.  
Starting dictionary attack. Please be patient.
```

```
The PSK is "family movie night".
```

```
4087 passphrases tested in 59.29 seconds: 68.93 passphrases/second  
$
```

Good reason to requisition a new laptop!

Enterprise WPA

- TKIP algorithm with 802.1x key distribution
- EAPOL-Key messages distribute encrypted keys following authentication
- Pairwise Master Key (PMK/256 bit)
 - Protects and generates PTK with random data
- Pairwise Transient Key (PTK/512 bit)
 - Split up into encryption keys, integrity keys and key encryption keys
- Encryption keys rotated every 2^{16} packets

PEAP Authentication Attack

- Attacker obtains list of valid usernames through traffic sniffing
- Manually attempts repeated authentication
 - Using common weak passwords
- Authenticator silently ignores bad passwords
- Likely to enable failed authentication account lockout policies
- Could be leveraged for DoS attack

Identifying WLAN IPSec Networks

Passive Analysis Methods

- Kismet will identify ISAKMP traffic
- Post-processing Wireshark filters
 - Display ISAKMP traffic "isakmp"
 - UDP ports 500, 10000, 5150 common
- Lots of UDP traffic to one destination

Status

Found new probed network "AP" bssid 00:90:96:A4:0C:8B

ISAKMP Traffic, Exchange type: Informational - from 00:01:02:3D:A3:30

Found IP 192.168.1.81 for NewportM::00:06:25:43:59:77 via TCP

Found IP 192.168.1.81 for NewportM::00:06:25:43:59:77 via TCP

Battery: unavailable, AC power

Auditing IPSec WLAN Networks

- Directed toward traditional vulnerability assessment
- May need to overcome simple layer 2 security (static WEP, MAC filters)
- Passive analysis often exposes FW rules
 - Active analysis also possible, but slow
- Test integrity of exposed systems
 - Patch levels, configuration vulnerabilities

Auditing Implementation Weaknesses

- Test IPSec server for aggressive IKE
 - Scan systems with ike-scan, record
 - Post-process with Wireshark
- Test DNS for recursive name resolution
 - Establish a known TXT record

Wireshark Aggressive Mode Filter: "isakmp[18] eq 4"

Check DNS recursion: "dig @remote-dns IN TXT hostname"

Making Wireless Pentests Valuable

- Wireless access is acquired
 - Now use classic network and application pentest techniques
 - Identify specific vulnerabilities and potential damage/risk
 - Change equipment and policies to limit the risk as much as possible
 - Rinse and repeat